UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
18978 NORTHERN DANCER LANE, YORBA LINDA, CA, 92886

Case No. 2:18-MJ-02516

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1028A, 1344, 1349, and 1956	See attached Affidavit

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Kathryn Bailey
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and state: Los Angeles, California

Hon. Patrick J. Walsh, Chief Magistrate Judge
Printed name and title

AUSA Andrew Brown, x0102, 11th Floor

ATTACHMENT A: 18978 NORTHERN DANCER LANE

The premises to be searched is:

18978 NORTHERN DANCER LANE, YORBA LINDA, CA 92886 (HOME OF LU AND HUNG). HOME OF LU AND HUNG is a two-story townhome located on NORTHERN DANCER LANE in the San Lorenzo community of the city of Yorba Linda. The entrance to the San Lorenzo community is located at the cross streets of Bastanchury and Emerald Downs. The HOME OF LU AND HUNG is attached to another home. The HOME OF LU AND HUNG is approximately 2200 square feet and consists of three bedrooms and three and half bathrooms. The 2nd floor has a walk out balcony that overlooks Northern Dancer Lane. The exterior of the home is a combination of red brick, white stucco, beige side paneling, and a grey tiled roof. The front entry is a single brown door with two windows in the door and the number 18978 affixed to the wall on the right side of the door. The premises to be searched includes an attached two-car garage and the vehicles within it.

ATTACHMENT B (Hung & Lu)

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 1028A, 1344, 1349, and 1956, namely:

a. Mail matter and shipping packages, opened or unopened, not addressed to or from 18978 NORTHERN DANCER LANE, YORBA LINDA, CA 92886 (the "HOME OF LU AND HUNG");

b. Personal identifying information of individuals other than YU HAO HUNG, aka "Alex Young," and TI LU, aka "Deer Lu," aka "Jerry Young," and others residing at the premises being searched, including social security numbers, dates of birth, addresses and telephone numbers, credit, gift, or debit card information, credit reports, and bank or other financial institution information, and records referring or relating to such information including transactions conducted in the names of those individuals;

c. Precious metal coins, ingots, and bars, such as those made of gold, silver, or platinum, and records referring or relating to precious metals;

d. Documents and records referring or relating to the following identities: Julian Chang, Henry Chen, Erin Cho, Andy Chu, Allison Kawai, Sydney Fu, Andran Ghaghian, Sahak Ghagian, Thomas Hayata, Chia-Hui Hung, Pat Jang, Cory Kang, Max Kao, Henry Koren, Paul Koren, Jamie Kwan, Daniel Lao, Casey Lee, Jack Lee, Gabby Li, Kris Lim , Terry Long, Peter Lu, Gale Ma, Reese Neho, Chris Pan, Alex Park, Autumn Ray, John Ray, Yevgenya Sayadyan, Taylor Song, Ricky Su, Drew Sun, Jackie Tang, Terry Tao, Steve Wang, Sam Wu, and Morgan Zhang;

e. Records relating to TLO and other databases of personal identifying information, credit applications, tradelines, adding and removing authorized users to a credit card account, and

other techniques to manipulate credit scores, including disputing negative credit information, and credit repair;

f. Records, programs, and items relating to the counterfeiting or manipulation of documents and identifications, such as the cutting-and-pasting of signatures, forging or copying of checks, passports, driver's licenses, and other form of identification, identification-proportioned photographs of faces, letterheads, watermarks, and seals, including the altered or counterfeited information itself.

g. Records relating to wealth and the movement of wealth since January 2003, such as brokerage and financial institution statements, wire transfers, currency exchanges, deposit slips, cashier's checks, and/or other financial documents related to depository bank accounts, lines of credit, credit card accounts, real estate mortgage initial purchase loans or loan refinances, residential property leases, escrow accounts, the purchase, sale, or leasing of automobiles or real estate, or auto loans, and investments, or showing or referring to purchases or transactions for more than $10,000, including any records referring or relating to NV Acquisition Management or Giovanni Fernandez, or business entities owned or controlled by NV Acquisition Management or Giovanni Fernandez;

h. Merchant account terminals and magnetic card readers, records, documents, programs, applications or materials relating to them or businesses that provide merchant processing services such as Elavon, Bank of America Merchant Services, and First Data;

i. Records referring or relating to trusts or business entities owned or controlled by YU HAO HUNG, aka "Alex Young," aka "Allison Kawai," or TI LU, aka "Deer Lu," aka "Jen Lu," aka "Jerry Young," including AMAT Diversified Inc., AMK Group, Belle Corp., Belle Nova Trust, De-Ani Inc., Gold World Inc., Nova Belle Trust, Nova Diversified, NDC Designs, Platinum Holdings, Roxbury Management Inc., Symphony Enterprises, and Vintage Reproductions;

j. Records or items containing indicia of occupancy, residency or ownership of any location or vehicle being searched, such as leases, utility bills, identity documents, and cancelled mail including those relating to 18978 Northern Dancer Drive, Yorba Linda, CA 92886, a silver 2006 Mercedes with California plate number 6KQH342, and a grey 2007 Honda Odyssey, California plate number 5YUV970;

k. Digital currency and prepaid debit or gift cards, and related documents and programs, and currency if the currency's value in total exceeds $1,000;

l. Documents and keys relating to public storage units, rental cars, safety deposit boxes, Commercial Mail Receiving Agencies, building or office space, or receiving mail at someone else's address including 613 Alderbery Lane, Pomona CA 91767;

m. Documents and records showing email and telephone contacts and numbers called, such as SIM cards, address books, call histories, and telephone bills;

n. Documents and records referring or relating to law enforcement or financial institution investigations, including accounts which were closed involuntarily by a financial institution, or to hiding money, storing funds abroad, or evading taxes or reporting requirements;

o. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

p. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to

control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such

as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES1

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant

1 August 10, 2017, protocol for digital devices not in custody with biometric unlocking only for named conspirators.

to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "Nuix," "EnCase," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while

an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. If YU HAO HUNG, TI LU, or Allen Lu is located at the premises being searched and is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device found there that falls within the scope of the warrant, then law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of the person onto the fingerprint sensor of the device

(only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of the person with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any other search of the digital devices.

AFFIDAVIT

I, Kathryn Bailey, being duly sworn, declare and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since January 2016. I am currently assigned to a Los Angeles Field Division White Collar Crimes Squad, which is responsible for investigating financial institution fraud, including bank fraud and wire fraud. My position has vested me with the authority to investigate violations of Federal Criminal law, to include, but not limited to, wire fraud and financial institution fraud. Prior to being employed by the FBI as a Special Agent, I was employed as a certified public accountant.

2. As a Special Agent with the FBI I have investigated various types of financial crimes, including wire fraud, money laundering, bankruptcy fraud, identity theft and various types of financial institution fraud. I have participated in many aspects of criminal investigations including, interviews, reviewing evidence, conducting physical and electronic surveillance, and the execution of search and arrest warrants. I have received formal advanced training in investigating crimes such as bankruptcy fraud, money laundering and various other financial frauds. In addition, I attended New Agent Training at the FBI Academy in Quantico, Virginia where I received extensive instruction in FBI core mission areas, legal authorities, laboratory techniques, as well as intelligence related to the criminal mission sets.

SEARCH WARRANTS AND PREMISES TO BE SEARCHED

3. I make this affidavit in support of applications for search warrants for evidence of suspected violations of Title 18 United States Code, Sections 1349 (Conspiracy to Commit Bank fraud), 1344 (Bank Fraud), 1028A (Aggravated Identity Theft) and 1956 (Laundering of Monetary Instruments) at the following premises (collectively, the "SUBJECT PREMISES"):

a. 18978 NORTHERN DANCER LANE, YORBA LINDA, CA, 92886 (the "HOME OF LU AND HUNG") (described with more particularity in Attachment A), the principle residence of TI LU and YU HAO HUNG and the principle location from where the aforementioned crimes are perpetrated as described in this affidavit.

b. The 2006 SILVER MERCEDES with license plate 6KQH342, and Vehicle Identification Number (VIN) WDBUF26J26A870149, registered to Allison Kawai (an alias for YU HAO HUNG) at 14556 Rice Ave. Chino, California 91710 ("HUNG'S MERCEDES"). The subjects used this vehicle to transport evidence of the crimes as described further in this affidavit.

c. The 2007 GREY HONDA ODYSSEY with license plate 5YUV970, VIN 5FNRL38707B433539, registered to Allison Kawai (an alias for YU HAO HUNG), at 324 S. Diamond Bar Blvd. #357, Diamond Bar California 91765 ("HUNG'S ODYSSEY"). This vehicle was used by the subjects as described further in this affidavit.

d. SAFETY DEPOSIT BOX 751, located at Chase Bank, 270 S. State College Blvd., Brea, CA 92821, held in the name of Nova Belle Trust, account number #-5197, 06X10 in size, with Alex Young identified as the trustee ("HUNG'S SAFETY DEPOSIT BOX"). Alex Young is an alias of YU HAO HUNG. TI LU and YU HAO HUNG store gold and

other valuables purchased using fraudulent proceeds in the safety deposit box as described later in this affidavit.

e. 613 ALDERBERY LANE, POMONA, CA 91767 (described with more particularity in attachment A) which is the residence of TI LU's brother, Allen Lu ("LU'S BROTHER'S HOME"). 613 ALDERBERY LANE, POMONA, CA 91767 was used as an address to open fraudulent depository bank accounts and lines of credit and to receive mail for many of the fraudulent accounts as described in this affidavit.

ASSET SEIZURE WARRANTS: LINKS BETWEEN ACCOUNTS AND DEFENDANTS

4. This affidavit is also made in support of seizure warrants for the following bank, brokerage, and investment accounts controlled by defendants TI LU and YU HAO HUNG (collectively, the "SEIZABLE ACCOUNTS"):

	Account Name	Financial Institution	Balance as of date:	Account Type	Account Number	Balance	See Paragraph
1	Ti Lu	TD Ameritrade	5/31/2017	Investment	754-891251	$265,000	7, 56, 72
2	Jen Lu	TD Ameritrade	5/31/2017	Investment	754-382455	143,000	7, 72
3	Nova Diversified Corp DBA NDC Designs	Bank of America	9/18/17	Checking account	501009452585	277,785	5, 18, 54, 57, 61, 62
4	Allison Kawai	Bank of America	9/18/17	Checking account	325072566370	18,420	6, 58
5	Nova Belle Trust	Bank of America	9/18/17	Checking account	000205266404	9,523	5, 63, 64
6	Nova Diversified Corp	Wells Fargo	1/31/18	Checking account	9015689558	84,212	5, 18, 40, 53, 59, 60, 61
7	Nova Diversified Corp	Wells Fargo	1/31/18	Savings account	1659652646	1,804	5, 59
8	NV Acquisition Management, LLC	Bank of America	1/31/18	Investment	N/A	$1,062,500	49, 60
	Total Cash and Investments					**$1,862,244**	

5. The following Bank of America and Wells Fargo bank accounts are associated with YU HAO HUNG through the use of her name "Alex

Young" as the signor on each of these accounts: Bank of America accounts in the name of Nova Diversified and Nova Belle Trust, accounts ending **501009452585** and **000205266404**, respectively, and Wells Fargo account in the name of Nova Diversified, accounts ending **9015689558** and **1659652646**. YU HAO HUNG opened all of the accounts, with the exception of the Nova Belle Trust Bank of America account, using her Alex Young California Driver's License, number D3570503. Alex Young is a known alias for YU HAO HUNG. I examined the photograph on California Driver's License D3570503, in the name of Alex Young, and it is a photograph of YU HAO HUNG. The opening documents for the Nova Belle trust account included a signature of Alex Young as Trustee. The Nova Belle Trust also owns TI LU and YU HAO HUNG's residence, 18978 NORTHERN DANCER LANE, YORBA LINDA, CA. Refer to paragraphs 63 and 64 for further information on the fraudulent use of the Nova Belle Trust Bank of America account.

6. The Bank of America account **325072566370** is held in YU HAO HUNG's alias "Allison Kawai." I examined the photograph for California Driver's License number D1089182, in the name of "Allison Kawai," and it is a photograph of YU HAO HUNG. In addition, the address on both accounts is at a commercial mail receiving agency (CMRA) that I have observed TI LU enter to retrieve mail.

7. The TD Ameritrade account **754-382455** in the name of "Jen Lu," an alias of TI LU, was also associated to TI LU and YU HAO HUNG through the IP address used to apply for the account. The IP address resolved back to Yorba Linda (where the HOME OF LU AND HUNG is located), and the specific IP address, 172.88.220.102, was also used to open the TD Ameritrade account in the name of TI LU, account **754-891251**.

INDICTMENT WITH FOREITURE ALLEGATIONS INCORPORATED

8. The Grand Jury indicted defendants TI LU, also known as ("aka") "Deer Lu," aka "Jen Lu," aka "Allen Lu," and aka "Jerry Young," and YU HAO HUNG, aka "Alex Young," aka "Allison Kawai", aka "Charlene" ("defendants") for conspiracy to commit bank fraud, aggravated identity theft, and conspiracy to launder money, on September 14, 2018. The indictment also contained forfeiture allegations against many of the defendants' bank, brokerage, and investment accounts, including all of the ones which this affidavit seeks seizure warrants for. The indictment is incorporated by reference. AUSA Andrew Brown informed me that the Ninth Circuit held in United States v. Seybold, 726 F.2d 502, 504-05 (1983), that magistrates may consider the information contained in an indictment in making a subsequent probable cause determination.

SYNTHETIC IDENTITY CREDIT CARD BUST OUT SCHEMES

9. Based on my knowledge, training, and experience, as well as information related to me by other special agents, I know that:

10. Synthetic identities involve combining pieces of personal identifiable information of real individuals with a valid, but unrelated, social security number. The various identifiers, to include name, date of birth, home address, phone number, and email address, are combined with the valid social security number in order to begin the process of building a credit history.

11. Once a synthetic identity is created, a public record of the identity is formed by opening utility accounts, establishing lines of credit, obtaining credit cards, and adding the synthetic identity as an authorized user on an account with an established

positive credit history and rating. This results in the synthetic identity appearing to have a legitimate credit history, with a favorable credit rating.

12. After the synthetic identity has a favorable credit rating, lines of credit are obtained from financial institutions. In my experience this is often accomplished simultaneously with opening a checking account. With a public record and a favorable credit rating, the synthetic identities are then used to obtain high credit card limits. This allows the "bust-out" activity to occur.

13. In my experience, the perpetrators will purchase "throw away" phones, each with a different phone number, for use with each synthetic identity created. The perpetrator's personal phone is used to communicate with other individuals involved in the scheme and, at times, to track various financial account, or related, information.

14. "Bust-out" activity takes place when the synthetic identity's credit card is used to make purchases and other high dollar charges in a short time frame. The purchases and other charges continue until the credit card limit is reached or the financial institution suspends the credit card. Once the limit is reached, a payment for the balance will be made to the credit account using a check drawn on a bank account in the name of the synthetic identity. This bank account will have little to no money in it, a fact known to the perpetrator. Once the payment is received, credit is immediately made available, allowing the perpetrator to start the process again, effectively doubling or tripling the credit originally available on the account. This is often referred to as the second and third phases of the scheme. After the "bust-out" activity occurs, very little to no effort is made to repay the outstanding

balance. Ultimately, the accounts are often charged off as bad debts or credit risk by the financial institutions, which may not realize that they have been defrauded.

15. In my experience I have observed that, in order to further the scheme, some perpetrators will also create fake businesses. The perpetrators apply for a merchant terminal for the fake business through a financial institution or third party vendor. The perpetrator will then swipe the credit cards obtained using the synthetic identities through the merchant terminal associated with the fake business. This helps to accelerate the "bust-out" by having a point of sale readily available. Based on my training and experience, the perpetrators will sometimes carry the merchant terminals and cell phones with them while outside their residence. Some of the merchant terminals require a cell phone to work properly.

16. The proceeds from the credit card swipes on these merchant terminals are deposited into bank accounts designated by the perpetrator when opening a merchant account. In my experience these funds are then moved from the depository account into another linked account. Checks are written from the linked account to various real and synthetic identities that are controlled by the perpetrator and deposited into intermediate bank accounts. By doing so, the funds are laundered through several layers of accounts.

SUMMARY OF THE SCHEME

17. TI LU and YU HAO HUNG are synthetic identity bust-out perpetrators. TI LU and YU HAO HUNG find social security numbers that are not being actively used and attach a name and birthday to that identity. A favorable credit rating for the synthetic identity is then built up using the methods described in the previous section.

With a strong credit rating established, TI LU and YU HAU HUNG apply for several lines of credit using the newly created synthetic identity. TI LU and YU HAO HUNG then plan for a time to execute the bust out scheme, usually around a 3-day or 4-day weekend so the TI LU and YU HAO HUNG can maximize their proceeds using the methods described in the previous section. In my experience, busting out credit cards on a long weekend helps ensure that a second and third phase of the bust-out scheme can take place given banks are typically closed on holidays and the financial institution's computer system will automatically provide credit upon any receipt of payment.

18. The fraudulent proceeds are transferred between several different bank accounts under different names of individuals, trusts, and corporations. In this case, some of those accounts include the Bank of America Nova Diversified account, **501009452585**, the Wells Fargo Nova Diversified account, **9015689558**, and the Bank of America Gold World Inc. account -9638, closed as of 8/9/17 per information provided by Bank of America. Proceeds are used to purchase gold, gift cards, real estate, and other investments.

19. TI LU and YU HAO HUNG typically bust out an identity over the course of a weekend and then take time off from their fraud before starting the process again. As described in more detail later, the investigation has indicated that the TI LU and YU HAO HUNG have been working this scheme for many years, probably more than 15.

20. YU HAO HUNG stated on July 30, 2017 that she could make about $200,000 using two individual names as part of the normal operations of the scheme. Although the bank records we obtained in this investigation are mostly restricted to 2014-2018, we nonetheless

found approximately 60 separate identities linked to TI LU and YU HAO HUNG. These identities include individuals and corporate entities.

FACTS SUPPORTING PROBABLE CAUSE TO SEARCH

21. The Federal Bureau of Investigation (FBI) received information on March 24, 2017 from Bank of America Investigator James Chaves indicating a particular bank insider had opened fraudulent accounts using synthetic identities. Some of these accounts came back to addresses in Pomona, California and had connections to addresses in Yorba Linda, California (where the HOME OF LU AND HUNG is located). The names on some of these accounts were TI LU, Jerry Young, Alex Young, and Bella Nova Trust, among others. A cooperating witness (CW) separately told the FBI that TI LU and his wife YU HAO HUNG are involved in credit card bust-out fraud.

22. The cooperating witness (CW) in this case was a professional credit card fraudster like TI LU and YU HAO HUNG. CW began cooperating with the FBI after being confronted with evidence of CW's guilt. CW is cooperating in hopes of a less severe sentence. In the course of this investigation, I, and other agents, have attempted to corroborate or disprove CW's statements many times. In each instance, where we have been able to do so, we learned that the information CW provided was accurate. To my knowledge, CW has never lied to the FBI while cooperating.

23. In addition to the report provided by Bank of America, the FBI received other financial information from Bank of America, and various other financial institutions, related to the accounts linked to TI LU and YU HAO HUNG. Based on my experience in investigating the use of synthetic identities and credit card bust-outs, the activity in the accounts appears to be that of a bust-out scheme.

Through review of the information provided by the financial institutions, I could identify the credit card swipes used by certain merchant terminals and see the immediate subsequent transfer of funds to another known fraudulent account. Refer to paragraphs 52 through 64 for an analysis of the movement of funds.

TI LU agreed to run fraudulent credit cards through his mobile merchant terminals

24. On March 27, 2017, a recorded phone call was placed from CW to TI LU's cell phone number 714-388-5761. Investigators know the number to be LU's because the number is listed in databases as belonging to TI LU and his wife YU HAO HUNG (under aliases Jerry Young and Alex Young). It is also the same number listed as the contact number for at least one of LU's accounts. During the call, TI LU offered his merchant terminal to CW to use to swipe certain fraudulent credit cards. I listened to the recording in which TI LU and CW discussed (1) how many credit cards CW would run through the merchant terminals (2) how many merchant terminals TI LU should bring and (3) for how much each credit card would be processed. TI LU and CW also discussed if a mutual acquaintance, Oscar, had anyone else at the bank. I learned through listening to subsequent recordings between TI LU and CW, that Oscar previously worked at a financial institution and had helped TI LU open fraudulent bank accounts and obtain credit lines. TI LU discussed having to get another bank insider because Oscar no longer worked at a financial institution in that capacity.

TI LU drove HUNG'S MERCEDES to pick up mail at an address used on fraudulent credit applications

25. On March 30, 2017, Special Agents (SAs) of the FBI Los Angeles Field office conducted a surveillance starting at 300 S. Diamond Bar Blvd in Diamond Bar, California, the location agreed upon by TI LU to meet CW to run three separate fraudulent credit cards through TI LU's mobile merchant services terminals. TI LU entered the parking lot in a SILVER MERCEDES, license plate 6KQH342 (HUNG'S MERCEDES). TI LU was observed by FBI SAs exiting a Postnet Mail Store, 324 S. Diamond Bar Boulevard, Diamond Bar, CA, which is an address used on certain synthetic IDs employed by TI LU and YU HAO HUNG when applying for credit lines.

26. TI LU transported merchant terminals in a briefcase to a meeting to swipe fraudulent credit cards. TI LU was observed by FBI SAs exiting his vehicle, carrying a briefcase, and entering the vehicle of CW. The audio and visual of the meeting between TI LU and CW was recorded. Through review of the recording, I witnessed two attempts to swipe the fraudulent credit cards brought to the meeting by CW. Each swipe was declined.

27. Through listening to the recording of the March 30, 2017 meeting, I learned that TI LU and CW discussed whether the credit cards CW brought were from "ghost" files or "real people" files. Ghost files are synthetic identities. I also heard TI LU agree to a 30% cut for allowing CW to use TI LU's merchant terminals to process the credit card transactions. Additionally, I heard TI LU collaborate with CW on what dollar amounts to charge on each card prior to swiping through the merchant terminal. Lastly, the recording captured TI LU's discussion on finding social security numbers ("numbers") for the ghost files. TI LU expressed to CW that he was not going to worry about the social security numbers; that the numbers were not

difficult to obtain. TI LU indicated he could always get numbers if CW needed them.

TI LU drove the HUNG'S MERCEDES to Chase Bank to meet a corrupt bank insider

28. FBI SAs observed TI LU enter a JP Morgan Chase Bank branch located at 2500 E. Imperial Highway, Brea, California. An FBI SA observed TI LU meet with a bank employee. CW indicated that the purpose of this meeting was for TI LU to introduce himself to a bank insider that could possibly help TI LU to continue the scheme. I listened to subsequent recorded phone calls between TI LU and CW where TI LU indicated this bank employee, Justin, was opening up checking accounts and helping TI LU obtain credit lines using synthetic identities. TI LU paid Justin 10% of the credit limit the identities were approved for.

TI LU drove the merchant terminals in HUNG'S MERCEDES to the HOME OF HUNG AND LU

29. After exiting the bank branch, FBI SAs followed and observed TI LU pull into the garage of 18978 NORTHERN DANCER LANE, YORBA LINDA, CA, a house shared with his wife, YU HAO HUNG, and daughter ("HOME OF HUNG AND LU"). According to property records the HOME OF HUNG AND LU is owned by the Nova Belle Trust with Alex Young (an alias of YU HAO HUNG) named as the trustee.

YU HAO HUNG and TI LU drove HUNG'S ODYSSEY to a meeting in which they discussed opening two new credit files using fraudulent identities

30. I viewed the video and audio of a recorded meeting on March 30, 2017, that CW had with TI LU and YU HAO HUNG. In the recording,

YU HAO HUNG suggested CW put the address 18978 NORTHERN DANCER LANE, YORBA LINDA, CA (the HOME OF HUNG AND LU) on the driver's licenses of two individuals that were planning to sell their identity information to CW for fraud. On the recording YU HAO HUNG was heard listing current credit cards she has that could be used for the new files. In my training and experience, as part of bust-out schemes, it is common to add new files, whether synthetic or not, as authorized users to aged credit accounts. This allows the new files to use the good credit history from the established account. In the recording, I heard YU HAO HUNG list certain credit cards she had, including the issuers, the credit limits, and how long she has had the credit cards. YU HAO HUNG followed up the conversation with a text message to CW listing the credit card information, which I viewed. Captured in the recording, YU HAO HUNG suggested moving the addresses associated with the credit cards to 18978 NORTHERN DANCER LANE, YORBA LINDA, CA (HOME OF HUNG AND LU) from 613 ALDERBERY LANE, POMONA, CA (LU'S BROTHER'S HOME). On the recording, YU HAO HUNG said they could make about $200,000 using the two new files. YU HAO HUNG stated she had a merchant terminal at Bank of America that had no limit for transactions.

31. **YU HAO HUNG was worried law enforcement would show up at 18978 NORTHERN DANCER LANE, YORBA LINDA, CA**. I listened to a recorded call dated 8/29/2017 and in it, TI LU, YU HAO HUNG and CW discussed what would happen if law enforcement came to 18978 NORTHERN DANCER LANE, YORBA LINDA, CA and knocked on the door. In the recording, I

heard TI LU state that Charlene keeps worrying. Charlene is an alias for YU HAO HUNG. YU HAO HUNG then commented that, "there is a kid here, that's why I'm worried." TI LU stated they do not have to worry about the issue right now and YU HAO HUNG interjected "we have to".

TI LU and YU HAO HUNG run their fraud from a room in the HOME OF HUNG AND LU

32. According to CW, TI LU and YU HAO HUNG run their fraudulent activities out of a home office located on the second floor of their home at 18978 NORTHERN DANCER LANE, YORBA LINDA, CA. CW stated that the files for the synthetic IDs are located in that office along with the merchant terminals and the digital devices used to access the accounts at the banks and TLO. TLO is a search tool used by TransUnion that examines public and proprietary records for information. TLO provided information that included the IP addresses used to log into the account owned by TI LU. An IP address that was used to log in to TI LU's TLO account is the same IP address that was used to create the TD Ameritrade account in TI LU and JEN LU's name, and to apply on-line for lines of credit using a synthetic identity, Reese Niho, as described in more detail below. I observed TI LU drive the merchant terminals in HUNG'S MERCEDES, license plate 5YUV970, to his residence at 18978 NORTHERN DANCER LANE, YORBA LINDA, CA. YU HAO HUNG confirmed the TLO account was still open and active in a recorded phone conversation with CW on 11/9/17.

33. In a recorded phone call between TI LU and CW on 8/29/17, TI LU discussed not wanting to log into a bank account from home (the HOME OF HUNG AND LU) because he did not want so many IPs coming back to the house. TI LU decided to log in to the bank account using his cell phone instead.

34. In a recorded phone call between TI LU and CW on 9/4/2017, TI LU told CW that there was a geolocation and IP stamp recorded when cards are swiped through his merchant terminal. He said most of the IP stamps resolve back to his house (the HOME OF HUNG AND LU) and it had not caused a problem. Sometimes, however, TI LU liked to drive to neighboring cities to do the swipes so it does not always show charges at his house.

35. In a recorded call dated 11/9/17 between YU HAO HUNG and CW, CW suggested YU HAO HUNG change the location of certain synthetic identities to 18978 NORTHERN DANCER LANE, YORBA LINDA, CA to possibly get more preapproved offers on credit cards YU HAO HUNG was applying for. YU HAO HUNG stated she did not want to jeopardize the house where her family lives, especially with her daughter there.

TI LU and YU HAO HUNG support their family through fraud

36. TI LU and YU HAO HUNG do not have any legitimate employment history. The Employment Development Department does not have any record of employment for TI LU and YU HAO HUNG or any of their known aliases. In addition, I listened to a recording dated 8/29/17 in which TI LU confirmed the last job he had was in commercial real estate before he met CW. TI LU and YU HAO HUNG have known CW for approximately 15 years. TI LU had the phone on speakerphone during this recorded call so YU HAO HUNG could hear the conversation. TI LU, with input from YU HAO HUNG in the background, stated it had been a long time since they had legitimate jobs.

TI LU and YU HAO HUNG purchased gold with fraud proceeds

37. I reviewed credit card statements from a Bank of America account in the name of Roxbury Management, with credit card ending -1712, and the account included authorized user TI LU, credit card

ending -6562. Through review of these statements, I learned that gold was purchased at Panda America on 4/14/15 for approximately $7,000. This purchase was on credit card ending -6562. In addition, approximately $8,000 was purchased at Panda America on 8/31/17 with Chase credit card number ending in -8901 in the name Reese Niho, a synthetic identity used by TI LU and YU HAO HUNG.

TI LU said he purchased gold with fraudulent proceeds.

38. I listened to a recorded call dated 8/18/2017 in which TI LU referred to a credit card that had a balance of $11,300, a credit limit of $27,000, and said he needed to use the balance before the second and third phase (i.e., before making a bogus payment on the account to clear out the balance so the card could again be used for fraudulent purchases). TI LU stated he could pay some more bills, purchase prepaid visa cards, or purchase gold. A detailed discussion ensued on the purchase of gold from Kevork at Gold Depot. TI LU asked CW if Kevork would need a social security number or a Tax Identification Number from TI LU in order to allow the purchase of gold.

TI LU and YU HAO HUNG store the gold purchased with fraud proceeds in HUNG'S SAFETY DEPOSIT BOX

39. I listened to a recorded call dated 8/28/17 in which TI LU was planning with CW to go see "Kevork" to sell gold with YU HAO HUNG. The CW sold gold previously to Kevork Kacharian, owner of Gold Depot, Inc. in Los Angeles, located at 640 S Hill Street. TI LU and CW discussed on the recorded call that CW would go into the gold store with YU HAO HUNG. TI LU stated that before he and YU HAO HUNG came to pick up CW, they had to go to Chase Bank to get the gold because it was "not in our possession." TI LU explicitly stated the

gold was in a CHASE SAFETY DEPOSIT BOX. This call was on speaker phone with YU HAO HUNG, who in the background contributed to the conversation while they made plans, albeit unintelligibly on the recording.

TI LU and YU HAO HUNG laundered fraud proceeds through selling gold and put the proceeds into one of the SEIZABLE ACCOUNTS

40. According to CW, TI LU and YU HAO HUNG picked up CW at CW's residence and proceeded to drive to Gold Depot to sell one bar of gold. The bar of gold sold for approximately $40,000. YU HAO HUNG received a check, made out to known alias Alex Young, dated 8/28/17 and for $42,020.05, according to bank records. TI LU and YU HAO HUNG then drove with CW to a Wells Fargo Bank branch to deposit the check into an account in the name of Nova Diversified Corp, account **9015689558**, owned by Alex Young. Bank statements confirmed this deposit activity. I listened to a recorded telephone conversation dated 8/28/17 in which TI LU and CW, along with YU HAO HUNG in the background on speaker, discussed the logistics of picking CW up, and that CW would go with YU HAO HUNG.

TI LU discussed buying more gold

41. I listened to a phone call recorded on 8/31/17 and TI LU stated that, based on a conversation with the CEO, Panda American would allow TI LU to buy gold via the telephone. TI LU specifically referenced purchasing one-ounce Swiss gold bars. Based on my training and experience, and information obtained throughout the investigation, TI LU purchased the gold with a fraudulent credit card issued based on information from a synthetic identity.

TI LU's brother will get fraud proceeds for receiving mail related to the fraud at LU'S BROTHER'S HOME

42. I listened to a recorded phone call between TI LU and CW on 8/17/2017 in which TI LU discussed using his brother's home at 613 ALDERBERY LANE, POMONA, CA as the address for some of the synthetic identities. TI LU said he traveled to the home to retrieve the mail from the banks. In two separate recorded phone calls dated 8/31/2017, I heard TI LU state that he will "take care" of his brother by buying him a new $3,000 mattress in the "third phase" using a ghost file (i.e., after busting out the credit card twice and resetting the balance to zero by writing bad checks for the balance).

TI LU and YU HAO HUNG received credit cards in the synthetic identities "Reese Niho" and "Autumn Ray"

43. Chase Bank investigator, Robby Perry, provided account information for four credit cards issued by Chase Bank to Reese Niho (card numbers -1844, -8901, -8791, -6720) and one credit card issued to Autumn Ray (card number -5827). The credit card accounts were opened on 12/2/16, 5/17/17, 8/10/17, 8/16/17 and 8/11/17, respectively. All five of the credit cards utilized LU'S BROTHER'S HOME as the address. Autumn Ray's application had TI LU as an authorized user. Three of Reese Niho's applications, completed online, used an IP address that resolved back to YORBA LINDA, CA, where the HOME OF LU AND HUNG is located. One application for Reese Niho, credit card -8791, and the Autumn Ray application, credit card -5827, were applied for in a Chase Bank branch.

TI LU answered the phone as synthetic identity Autumn Ray

44. In a recorded phone call on 9/6/2017, I heard TI LU interrupt his conversation with CW to answer another phone that was ringing in the background. Upon answering that call, TI LU stated, "This is Autumn Ray speaking." TI LU also spoke the digits "5239,"

which are the last four of the SSN for the Autumn Ray identity. After ending the call related to Autumn Ray, TI LU stated that the call was from Capital One about the application. Based on information provided to me by a Capital One investigator, Geraldine Schmitt, Autumn Ray applied for a credit card in September 2017, with a social security number ending in -5239. In addition, I listened to a recorded call dated 10/3/2017 and TI LU again answered a secondary phone that rang and TI LU stated, "Yes, this is Autumn speaking."

Charges on the Reese Niho and Autumn Ray fraudulent credit cards were made at merchant terminals owned by YU HAO HUNG and TI LU

45. Chase Bank records for the Reese Niho and Autumn Ray credit cards show there was a total of approximately $68,000 in charges across four of the credit cards at a merchant named NDC Designs, merchant identification number 09289987. I listened to recordings dated 7/30/17 and 11/9/17 and YU HAO HUNG said she had a Bank of America merchant terminal and that Bank of America merchant services told her there was "no limit," meaning no maximum for transactions. Based on information provided by Bank of America, NDC Designs is a company owned by YU HAO HUNG and the terminal is owned by Bank of America. There were also two separate charges, made on credit cards -1844 and -8901 for a total of approximately $13,000 to AMK Group. Approximately $6,000 was charged on card -1844 on 7/17/2017. $7,000 was charged on card -8901 on 9/4/2017. Information provided by FirstData, AMK Group is owned by Allison Kawai, an alias for YU HAO HUNG.

A credit card in the name of synthetic identity Reese Niho was used at TI LU's and YU HAO HUNG's daughter's school.

46. There were two payments made with credit card -1844 in the name Reese Niho for a total of approximately $9,700 to "HeritageOakPrivateed." Heritage Oak is the private education school in Yorba Linda, California where TI LU and YU HAO HUNG's daughter attends school, according to school records.

TI LU swiped a business credit card linked to synthetic identity Reese Niho through a merchant terminal owned by YU HAO HUNG

47. Chase Bank records show a credit card was issued in the name of Care Fusion Systems (card -6720) which was tied to Reese Niho's account. Care Fusion Systems had the same social security number (-1181) and telephone (725-696-2625) in the account information as Reese Niho. The credit limit for the Care Fusion credit card was $18,000. One of the transactions for credit card -6720 was a $9,300 swipe at NDC Designs, owned by Alex Young, an alias for YU HAO HUNG, on 8/24/17. TI LU confirmed he was responsible for obtaining the business credit card and swiping it through the NDC Designs merchant terminal in a recorded call dated 8/24/17 to which I listened. In the recording, TI LU told CW that he got the business card for $18,000. TI LU indicated in the recording he was going to max the card out between "now and tomorrow." TI LU then stated, related to the same business card, that he was going to charge $9,300 on "my machine."

Bank accounts controlled by TI LU and YU HAO HUNG made fraudulent payments on the Reese Niho and Autumn Ray fraudulent credit cards

48. Information provided by the Chase Bank investigator indicated there was a total of approximately $155,000 purportedly paid on the Reese Niho and Autumn Ray credit cards -1844, -8901, -

6720, and -5827 made through July-September 2017. These payments were made from bank accounts that did not have sufficient funds to cover the payments, a scheme often used to trick the bank into reducing the balance so that more charges could be made on the credit cards. The payments came from three separate accounts. One Chase Bank account -6568, one EverBank account -6154 and one Ally Bank account -9028. The Chase Bank account, in the name of Reese Niho, was opened September 2016 at a Chase Bank branch and used LU'S BROTHER'S HOME as the address. On a recorded call dated 8/29/17, I heard TI LU and YU HAO HUNG say both of the applications for EverBank and Ally were approved. The payment history on the accounts indicate approximately $60,000 was paid and posted on 8/30/17 and 8/31/17 across the credit card accounts. I listened to a recording on 8/30/17 in which TI LU stated he paid $60,000 on the cards that day. On a recorded phone call dated 9/4/17, TI LU stated he and YU HAO HUNG looked at the numbers and proceeded to question the negative balances seen on credit cards based on payments he made from Ally Bank and EverBank. TI LU indicated one of the credit cards showed a negative $27,000 balance. Based on the information provided by the Chase Bank investigator, three separate $27,399 payments were made on credit card x8901. One on 8/30/17 from Ally Bank account -9028 and two on 9/3/17 from Ally Bank account -9028 and EverBank account -6154.

TI LU and YU HAO HUNG have sent over $1 million to an investment in Orlando that does not report to the IRS

49. In a recorded phone call dated 11/9/17, YU HAO HUNG told the CW that she and TI LU sent $850,000 to a "guy in Orlando". Information provided by Bank of America identified that the "guy in Orlando" is Giovanni Fernandez, owner of NV Acquisition Management

and other businesses. Bank records show that YU HAO HUNG and TI LU have sent multiple wires to NV Acquisitions over the course of a couple of years. YU HAO HUNG stated that Fernandez sends a dividend every time he closes a property; no one is reporting to the IRS; and the dividend is approximately a 10-15% return.

YU HAO HUNG traveled to Taiwan in February carrying credit cards linked to the SEIZABLE ACCOUNTS

50. Travel records show that on 2/1/18, YU HAO HUNG and her daughter traveled from Los Angeles, California to Taiwan. YU HAO HUNG returned on 2/5/18. Upon entry into the United States, YU HAO HUNG was stopped by Customs and Border Patrol for a secondary screening. In her possession, there was approximately $6000 in cash, Bank of America and Wells Fargo credit cards with the business name of Nova Diversified Corp; a Citi credit card in the name of Platinum Holdings; and a Bank of America credit card in the name of Nova Belle Trust, the accounts through which she laundered proceeds. The customs officer asked YU HAO HUNG about the credit cards and the corporations named on them. YU HAO HUNG initially explained that she had worked for the companies approximately 10 years earlier but that now YU HAO HUNG was a stay at home mother and wife. The customs officer asked follow up questions about why YU HAO HUNG would still have company credit cards from a company she worked at 10 years ago. YU HAO HUNG became “flustered” and could not give a clear answer about the origin of the cards. YU HAO HUNG then attempted to explain that she and her husband owned the companies for real estate investing. After getting more “flustered,” YU HAO HUNG told the customs officer that the corporations were set up for tax purposes at the instruction of her accountant. YU HAO HUNG could not explain the

purpose of the corporate cards and why she had them, and ultimately told the officer to talk to her accountant.

YU HAO HUNG said she did not want to get involved in the recruitment of bank insiders

51. I listened to a recording dated 11/9/17 between YU HAO HUNG and CW. YU HAO HUNG indicated that Justin at Chase Bank was not aware of TI LU's and YU HAO HUNG's real intentions. Justin believed the accounts were for real people. YU HAO HUNG stated she did not know Justin and Justin did not know her. YU HAO HUNG did not want to get involved in the relationship with Justin and asked "why should I get involved?"

FACTS SUPPORTING PROBABLE CAUSE FOR FORFEITURE OF CERTAIN BANK AND INVESTMENT ACCOUNTS

52. The investigation to date has identified 12 financial accounts belonging to TI LU and YU HAO HUNG under their aliases that hold cash and investments. Each of these accounts were used to store or move fraudulent funds. The generation of the fraudulent funds largely came from the use of six merchant terminal accounts opened and operated by TI LU and YU HAO HUNG. TI LU and YU HAO HUNG swipe credit cards obtained using the methods described in the background section of this affidavit, through the merchant terminals. The revenue generated is processed into the associated bank account identified when the merchant account was opened. TI LU and YU HAO HUNG then manage the flow of money through various open bank and investment accounts.

Fraud proceeds were deposited into the Roxbury Management Wells Fargo account -0118 and laundered through Nova Diversified Wells

Fargo account 9015689558 and Roxbury Management Wells Fargo account ending -9120.

53. Symphony Enterprises is one merchant account opened by TI LU. Elavon, the merchant services provider for Symphony, provided information identifying the account holder as Jerry Young, an alias for TI LU. The total amount generated through the terminal was approximately $93,000. The bank account identified by TI LU on the application was a Wells Fargo account -0118. The name of that account is Roxbury Management Inc / Symphony Enterprises and was opened by TI LU in March 2015. We traced approximately $93,000 into the Wells Fargo account -0118 for the period of April 2015. TI LU then moved approximately $74,000 from Wells Fargo account -0118 to a Wells Fargo account **9015689558**. The Wells Fargo account **9015689558** is in the name of Nova Diversified Corp, dba Platinum Holdings and the account holder is Alex Young. From the Symphony Enterprises Wells Fargo account -0118, TI LU wrote checks in the amounts of $22,000 (dated 4/10/15), $22,900 (dated 4/13/15), $9,890 (dated 4/17/15) and $18,790 (check number 1001, dated 4/20/15) to Platinum Holdings, Wells Fargo account **9015689558**. Elavon closed the Symphony Enterprises merchant account in May 2015 due to identified bust out activity. Wells Fargo bank closed the account -0118 in July 2015. The Nova Diversified Corp Wells Fargo account **9015689558** remains active and maintains a balance as of 9/17/18.

Fraud proceeds were deposited into the Gold World, Inc. Bank of America account -9638 and laundered through Nova Diversified Bank of America account 501009452585.

54. Vintage Productions is a merchant account opened through Elavon in February 2015 for Paul Lu, TI LU's brother, and closed by

Elavon in June 2015 due to fraudulent activity. The bank account identified on the opening application was a Bank of America account -9638 in the name of Gold World Inc. dba Vintage Reproductions, which bank records show TI LU opened. For the period of February 2015 through April 2015, TI LU and YU HAO HUNG swiped approximately $129,000 in credit cards through the Vintage Reproductions terminal. We traced the $129,000 to the respective bank statements for the Gold World Inc. Bank of America account -9638. TI LU wrote checks from the Bank of America account -9638 for a total of approximately $181,000 to the Nova Diversified Corp Bank of America account **501009452585**. In the month of April 2015, TI LU wrote the following three checks to Nova Diversified Corp, account **501009452585**: (1) $47,500 dated 4/13/15; (2) $38,200 on 4/15/15; (3) $16,700 on 4/20/15. We traced each of these checks into the respective bank statement for Nova Diversified Corp Bank of America account **501009452585**. Additionally, in March 2015, TI LU wrote six checks from the Bank of America account -9638 to the same Nova Diversified Bank of America account **501009452585** for approximately $64,000 in total.

TI LU and YU HAO HUNG laundered fraud proceeds through a Bank of America account 501008688208 in the name of TI LU

55. In April 2015, TI LU wrote five checks from the Gold World Inc. Bank of America account -9638 to a Bank of America account in the name of TI LU, account number -8208. The total amount of Gold World Inc. checks was approximately $133,000 in April 2015 alone, consisting of check numbers 1044, 1047, 1048, 1050 and 1051. We were able to trace the checks to the Bank of America account -8208.

TI LU and YU HAO HUNG funded their TD Ameritrade investment account 754-891251, in the name of TI LU, with fraud proceeds

56. In April 2015, TI LU wired a total $138,000 to the TD Ameritrade account, account number **754-891251** from the TI LU Bank of America account -8208. We traced the three ACH payments in the amounts of $53,000, $47,000 and $38,000 dated 4/13/15, 4/21/15 and 4/24/15, respectively into the TD Ameritrade account **754-891251**.

57. On 1/31/18, TI LU received a $95,000 wire into the TI LU Bank of America account -8208 from TD Ameritrade. On 2/7/18, a check was written from account -8208 to the Nova Diversified Corp Bank of America account **501009452585** in the amount of $87,000, check number 134, dated 2/7/18.

Fraud proceeds were deposited into the Bank of America account 325072566370 in the name of Allison Kawai.

58. AMK Group is another merchant account opened through First Data, credit card processing services. Allison Kawai, an alias of YU HAO HUNG, opened the account in June 2016. The bank account associated with AMK Group is a Bank of America account in the name of Allison Kawai, account number **325072566370**. From date of opening of the merchant account to 10/31/17, a total of approximately $27,000 was charged through the AMK Group merchant account, including the credit card charges belonging to synthetic identity Reese Niho, discussed above. The majority of the money remains in the Allison Kawai Bank of America account **325072566370**. There were Chase credit card bill payments in August 2017, as well as Discover credit card bill payments in September 2017 out of the account **325072566370**. There has been limited activity in the account. The balance as of 9/18/18 is $18,420.

Fraud proceeds were deposited into the Nova Diversified Wells Fargo account 9015689558 and laundered through the Nova Diversified Bank of America savings account 1659652646.

59. In June 2016, YU HAO HUNG opened a merchant account in the name of Platinum Holdings through Elavon. The bank account associated with this merchant account is a Wells Fargo account in the name of Nova Diversified Corp dba Platinum Holdings, account **9015689558**. From the date of opening of the merchant account, to March 2017, approximately $26,000 in transactions were processed through the merchant terminal. Elavon provided each transaction through the Platinum Holdings merchant terminal that we traced to the respective Nova Diversified Wells Fargo bank statement for account **9015689558**. YU HAO HUNG transferred the money coming into account **9015689558** to Nova Diversified Wells Fargo savings account **1659652646**. Account **1659652646** is the savings account associated with the Nova Diversified Wells Fargo account **9015689558**. In July 2016, YU HAO HUNG transferred approximately $25,000 from Wells Fargo account **9015689558** to Wells Fargo account **1659652646**. In August 2016, YU HAO HUNG transferred approximately $15,000 from Wells Fargo account **9015689558** to Wells Fargo account **1659652646**.

60. The Platinum Holdings merchant account was terminated by Elavon security in May 2017. Since that time, there has been little activity in the Nova Diversified Corp dba Platinum Holdings, Wells Fargo account **9015689558**. YU HAO HUNG and TI LU have continued to deposit certain checks into account **9015689558,** such as three checks from Gold Depot as a result of selling gold, as well as checks from various other accounts held by YU HAO HUNG and TI LU. These deposits funded the wire transfer of $250,000 to NV Acquisitions on 12/6/17.

Surveillance video identified YU HAO HUNG conducting certain transactions related to the Nova Diversified Wells Fargo account 9015689558 and the Nova Diversified Bank of America account 501009452585.

61. Wells Fargo provided surveillance video for three separate transactions related to the Nova Diversified Wells Fargo bank account **9015689558**. Although the Nova Diversified Wells Fargo bank account **9015689558** is in the name of Alex Young, the surveillance video identified YU HAO HUNG at a Wells Fargo teller window on 11/30/17 depositing a check (check #1069) into this account for $60,000 from the Nova Diversified Corp Bank of America account **501009452585**. The surveillance video also identified YU HAO HUNG at a Wells Fargo teller window on 12/15/17 and deposited a check (check #16028) from Gold Depot, paid to Alex Young, in the amount of approximately $80,536. YU HAO HUNG also deposited a check on 12/18/17 (check #16027) for approximately $80,536, from Gold Depot and made out to Alex Young as seen on the surveillance video. These deposits were all into account **9015689558**. TI LU was also present in the videos alongside YU HAO HUNG; however, YU HAO HUNG was the individual making the deposits. A Wells Fargo investigator confirmed Nova Diversified Wells Fargo bank account **9015689558** had minimal activity in 2018 as of 9/17/18 but that there was a balance in this account.

Fraud proceeds were deposited into the Nova Diversified Bank of America account 501009452585.

62. YU HAO HUNG opened another merchant account under the name Nova Diversified Corp, dba NDC Designs through Bank of America merchant services in September 2016. The bank account associated with the merchant account is a Bank of America account in the name of

Nova Diversified Corp, account number **501009452585**. Bank of America provided information related to the Nova Diversified Corp merchant account that identified a total of approximately $70,000 transactions through the merchant terminal from the time the merchant account was open through November 2017. We traced the August 2017 transactions provided by Bank of America, total of approximately $24,000, to the respective Nova Diversified Corp Bank of America statement for account **501009452585**. The majority of withdrawals and other debits from the Nova Diversified Bank of America account **501009452585** are credit card bill payments and annual life insurance payments to Legal & General America. The balance of Nova Diversified Corp Bank of America account **501009452585** as of 9/18/18 was approximately $278,000 with the most recent transaction occurring on 9/10/18.

Fraud proceeds were deposited into the Nova Belle Trust Bank of America account 000205266404.

63. YU HAO HUNG is the trustee of Nova Belle Trust. The Trust holds an account at Bank of America in the name of Nova Belle Trust, account **000205266404**. The deposits and other credits to the account were funded by other accounts owned by TI LU and YU HAO HUNG. On 3/4/15, $3,500 was deposited into account **000205266404** via check number 1035 written from the Gold World Bank of America account -9638. Nova Belle Trust Bank of America account **000205266404** also received three checks over 10 months from Allen Lu, TI LU's brother, residing at 613 ALDERBERY LANE, POMONA, CA. The three checks were written from a Bank of America account ending -7346 and consisted of the following that were deposited into account **000205266404**: check number 661, dated 11/26/15 for $3,000; check number 664, dated 12/30/15 for $800; and check number 681, dated 8/4/16 for $7,227.50.

TI LU and YU HAO HUNG use the fraud proceeds deposited into the Nova Belle Trust Bank of America account 000205266404 for daily living expenses.

64. YU HAO HUNG and TI LU used the Nova Belle Trust Bank of America account **000205266404** to pay for daily necessities, such as bills for gas, water, and electric and community fees, according to bank records. A Bank of America investigator confirmed the balance as of 9/18/18 is $9,523.46 and the most recent activity was on 9/17/18.

TI LU and YU HAO HUNG discussed fleeing to Taiwan if charged.

65. I listened to a recorded phone call between TI LU, YU HAO HUNG and CW on 8/29/2017 where TI LU and YU HAO HUNG discussed possibilities if law enforcement were to get involved. YU HAO HUNG indicated they had to worry at this time and TI LU stated he could leave the country; he could fly back to Taiwan. YU HAO HUNG was on speaker and did not contradict TI LU's statements.

66. I reviewed the Department of Justice's Office of International Affairs website and noted that the United States does not have an extradition treaty with Taiwan.

TI LU has changed his name twice since moving to the United States from Taiwan.

67. TI LU immigrated to the United States under the name TI LU on November 30, 1979, with his parents. TI LU changed his name by decree of the court to "Deer Lu" when he became a citizen on August 26th 1986 through United States Citizenship and Immigration Services. He then changed his name again to "Jerry Young" on September 11th, 2000, through the Los Angeles County Court system.

YU HAO HUNG has changed her name since moving to the United States from Taiwan.

68. YU HAU HUNG first entered the United States from Taiwan on January 1, 1993 as an F1 student. On September 18, 1995, HUNG was admitted as a H1B Temporary Alien Worker. HUNG became a permanent resident on April 24, 1997. On June 16, 2000, HUNG submitted a "Petition for Name Change" to change her name to Alex Young. HUNG is currently known to CW, and referred to by her husband, as Charlene.

YU HAO HUNG and TI LU changed names to avoid debt and fraudulent activity.

69. On the "Petition for Name Change", dated June 16, 2000, just above HUNG's signature is the statement "I certify that I am not seeking a change of name for any unlawful purpose, such as the avoidance of debt or evasion of law enforcement". Government documents dated March 7, 2000, indicate, however, that YU HAO HUNG and her "United States Citizen husband" had "applied for and received numerous loans with the intention of absconding with the funds". According to the report, among other institutions, HUNG and LU potentially owe $110,000 to Mandalay Bay Casino, $75,000 to Rio Casino, and $50,000 to MGM Casino. In my training and experience, perpetrators of fraud often change their names and operate under aliases in order to make it more difficult for law enforcement to track their activities and illicit wealth.

TI LU and YU HAO HUNG have multiple identities with associated identification, social security numbers, and mailing addresses.

70. Through financial institution records and reports, the investigation so far has revealed that there are approximately 52 individual synthetic identities associated with LU and HUNG. There are just as many social security numbers and dates of birth tied to these identities. From review of records, the investigation has

revealed that TI LU has a driver's license, number C5240635, as well as a US Passport (number 488030800) associated with the name Jerry Young and Taiwanese Passport (number 135090515) in the name of TI LU. YU HAO HUNG has a driver's license in the names of Alex Young (number D3570503) and a separate driver's license in the name of Allison Kawai (number D1089182), both with a picture of the same person. YU HAO HUNG also has a US Passport in the name of Alex Young, number 476117651.

TI LU and YU HAO HUNG have multiple bank accounts in names other than their own.

71. Through our investigation, we have identified approximately 25 bank accounts associated with TI LU or YU HAO HUNG. These accounts are associated to TI LU and YU HAO HUNG through the owner of the account, mailing addresses used on the account, or IP addresses. Due to the nature of this scheme and the investigation, new accounts are found all the time. There is no reason to believe that the investigation has found all of the accounts. In my training and experience, it is very likely that there are additional, unknown accounts that could hold large cash balances available to TI LU and YU HAO HUNG. TI LU and YU HAO HUNG have a safety deposit box at Chase Bank that contains gold, including gold bars and coins.

TI LU and YU HAO HUNG are both Chinese (Taiwanese) citizens and have brokerage accounts in foreign names and with foreign addresses.

72. Our investigation has identified two active TD Ameritrade brokerage accounts (account numbers **754-382455 and 754-891251**) in the names of Jen Lu and TI LU, respectively. Both accounts listed addresses located in Taiwan. YU HAO HUNG's entire family, except her

daughter and her husband (who said he could flee to Taiwan if discovered by law enforcement), lives overseas and she is still in contact with them. On 2/1/18, YU HAO HUNG traveled to Taiwan due to an illness in her family. TI LU has two brothers in the United States. Based on the recorded calls and surveillance conducted of them, it appears that TI LU and YU HAO HUNG have few friends or other family living in the United States.

Recent Fraud Activity

73. I listened to a recorded phone call dated 4/30/18 where TI LU discussed the status of an open file with CW. TI LU stated that the file has the address of the "valet guy". As discussed in other recordings I have listened to, TI LU and YU HAO HUNG pay cash to the individual that valets at their daughter's school to use his address for their files. TI LU stated on the call that he has two credit cards from Chase; one Chase Sapphire card with a $5,000 limit that and one Freedom Chase card with a $2,000 limit. TI LU stated he had applied online for the Sapphire card within the last two weeks. TI LU is using his brother, Paul Lu, as the parent for this file to build up the credit score for the file. TI LU told the CW that he needed money to buy a house.

74. I listened to a recorded call dated 8/20/18 and TI LU told CW that he was leaving on a trip to Barcelona, Spain that night. TI LU, his wife Charlene (YU HAO HUNG) and their daughter were going to stay in Barcelona for five nights and then go on a Mediterranean cruise. TI LU then confirmed he used a ghost file to purchase the cruise. TI LU confirmed on the recorded call that he has paid for two other cruises "like that." TI LU explained in detail to CW how to use a ghost file to pay for the cruise. TI LU stated that Royal Caribbean

is easy. TI LU paid for the base line cruise using a ghost file credit card online. Once the initial cruise was purchased, TI LU can also go online and add a bunch of other stuff, such as excursions, packages. When TI LU boards the boat, he uses his own identification card and credit card to check into the boat; however, the cruise and excursions were already paid for using a ghost file. TI LU also explained that he uses "on board credit" to pay for food and drinks. However, TI LU calls to purchase "on board credit" in increments, purchasing $2,000, $2,000, and then $2,500 for a total of $6,500 to be used for "on board credit". TI LU uses a ghost file to add "on board credit."

75. On a 9/4/18 recorded phone call, I heard TI LU discuss using his brother, Paul Lu, as a sponsor for other ghost files. TI LU stated Paul Lu's profile is still sponsoring a couple of the files but the ghost files don't come out too well, they do not earn that much. TI LU said the issue is that Chase bank closed out all Paul Lu's good big accounts, as well as Capital One a few years back. (In my training and experience, banks that detect blatant authorized user misconduct or other signs of fraud may close the credit card accounts involved). TI LU determined he would leave Paul Lu's file alone at this time.

76. Discover Bank provided information that indicated TI LU and YU HAO HUNG used synthetic identity Casey Lee to charge approximately $21,100 on credit card account number -4299 for the period January 3, 2018 through May 17, 2018. Casey Lee was at address 613 ALDERBERY LANE, POMONA, CALIFORNIA initially but the address subsequently changed to an address in Phoenix, Arizona. Some of the charges on the account included transactions at an AMK Group and Novadiversi PayPal

accounts. Novadiversi is a PayPal account owned and operated by YU HAO HUNG according to information provided by PayPal. YU HAO HUNG and TI LU operated a merchant terminal in the name of AMK GROUP through First Data merchant processor. All payments made on credit card ending -4299 were returned due to insufficient funds. Discover Bank closed the account -4299 due to fraudulent activity.

77. BBVA Compass Bank provided information that indicated Daniel Lao conducted a credit card fraud in the form of a bust out scheme totaling $15,000. This occurred between 3/9/18 and 5/11/18 on credit card -8871 opened on 3/9/18 in the name of Daniel Lao with a credit limit of $6,000. BBVA Compass reported that two large charges were for Novadiversi Las Vegas and AMK Group Diamond Bar. Based on information provided by PayPal and First Data, these are entities known to be owned and operated by YU HAO HUNG and TI LU. Daniel Lao is listed on the utilities for 613 ALDERBERY LANE, POMONA, CALIFORNIA.

78. Wells Fargo Bank provided information that Daniel Lao conducted a fraud scheme on credit card account -6976. On 3/25/18, Wells Fargo issued this credit card to Daniel Lao with a credit limit of $7,500. Total loss on the card was $13,284. A charge on the credit card was to a PayPal account in the name of JYTECHSERVI. The records I received from PayPal for account Novadiversi owned and operated by YU HAO HUNG included payments to a JYTECHSERVI. There was a charge on the credit card was for Royal Caribbean Cruises in the amount of $2,500, which agrees to the recorded conversation discussed above on 8/20/18 when TI LU bragged about how he used ghost files for the family cruise in Barcelona. All payments made on credit card -6976

were returned for insufficient funds. Wells Fargo ultimately closed the account due to the activity.

79. On 9/13/18, FBI observed TI LU driving HUNG'S MERCEDES, returning to HOME OF LU AND HUNG. Also on 9/13/18, FBI observed YU HAO HUNG driving from the HOME OF LU AND HUNG in HUNG'S ODYSSEY.

KNOWN IDENTITIES AND CORPORATE ENTITIES IDENTIFIED THROUGH

80. The investigation identified approximately 60 separate identities linked to TI LU and YU HAO HUNG. These identities include individuals and corporate entities. The following is a list of identities used by TI LU and YU HAO HUNG to perpetuate the fraud: Julian Chang, Henry Chen, Erin Cho, Andy Chu, Allison Kawai, Sydney Fu, Andran Ghaghian, Sahak Ghagian, Thomas Hayata, Chia-Hui Hung, Pat Jang, Cory Kang, Max Kao, Henry Koren, Paul Koren, Jamie Kwan, Daniel Lao, Casey Lee, Jack Lee, Gabby Li, Kris Lim, Terry Long, Peter Lu, Gale Ma, Reese Neho, Chris Pan, Alex Park, Autumn Ray, John Ray, Yevgenya Sayadyan, Taylor Song, Ricky Su, Drew Sun, Jackie Tang, Terry Tao, Steve Wang, Sam Wu, and Morgan Zhang.

81. The trusts or business entities owned or controlled by JERRY YOUNG and YU HAO HUNG identified during the investigation include AMAT Diversified Inc., AMK Group, Belle Corp., Belle Nova Trust, De-Ani Inc., Gold World Inc., Nova Belle Trust, Nova Diversified, NDC Designs, Platinum Holdings, Roxbury Management Inc., Symphony Enterprises, and Vintage Reproductions.

Training and Experience Regarding Fraud Evidence:

83. Based on my training and experience, and discussions with investigators who have over 10 years' experience, I know that individuals involved in identity theft schemes like this one must

keep evidence of their schemes, such contact information for their co-conspirators, lists of victim information and accounts used in the scheme, simply to keep the scheme going, and that even outdated evidence of the scheme will likely persist on digital devices.

84. Generally, perpetrators of identity theft schemes like to maintain this evidence close at hand and where it is safe, such as in their residences, automobiles, and, especially with smartphones, on their person. For larger or more sophisticated frauds, such as this one, participants often attempt to distance themselves from some of the incriminating evidence by renting public storage units or safety deposit boxes where they often keep the items they will not need immediate access to.

85. In my training and experience, synthetic identity bust-out schemes like this one are done for financial gain and to maintain a lifestyle which requires that the scheme continue indefinitely to support that lifestyle. Typically, such fraudsters do not stop until they are arrested. Typically they also use the same modus operandi, provided that it continues to be successful. Here, LU and HUNG have been remarkably stable, owning and living in the same house for over a decade and using mostly the same bank accounts for their fraud and money laundering. Because I have seen no evidence of legitimate income for them, they have no wage data at EDD, and in a conversation with the CW, TI LU admitted that it had been a long time since they had legitimate work, which in context was likely to be over 15 years, I believe that LU and HUNG are continuing their fraud and money laundering today and will continue to do so using the same methods that they have already found to be tried and true.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES

86. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have

specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a

hard drive, deleted, or viewed via the Internet.[1] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

[1] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregated from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregated from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A

substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

Request to Use Biometric Features to Unlock Digital Devices

87. Based on my training and experience, and knowledge of this investigation as discussed previously, I believe that digital devices, such as smartphones, will be found during the search.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID

sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary to unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's

Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

88. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

89. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

90. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual who is found at the SUBJECT PREMISES and reasonably believed by law enforcement to be a user of the device to unlock the device using biometric features in the same manner as discussed in the following paragraph.

91. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the SUBJECT PREMISES and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or

fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

92. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

CONCLUSION

Based on the foregoing, I submit there is probable cause to believe that evidence of violations of Title 18, United States Code, Sections 1349, 1344, 1028A, and 1956 will be found at the SUBJECT PREMISES, and that SEIZABLE ACCOUNTS constitute and are derived from proceeds traceable to those violations, and are therefore subject to seizure pursuant to 21 U.S.C. § 853(f), 18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), and 21 U.S.C. § 853, and that the SEIZABLE ACCOUNTS are also subject to seizure pursuant to 18 U.S.C. § 984.

Kathryn Bailey
Special Agent, FBI

Subscribed to and sworn before me
on September ___, 2018.

UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

June 2018 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. YU HAO HUNG, aka "Alex Young," aka "Allison Kawai," aka "Charlene," and TI LU, aka "Deer Lu," aka "Jen Lu," aka "Jerry Young," Defendants.	CR No. 18- I N D I C T M E N T [18 U.S.C. § 1349: Conspiracy to Commit Bank Fraud; 18 U.S.C. § 1028A: Aggravated Identity Theft; 18 U.S.C. § 1956(h): Conspiracy to Launder Money; 18 U.S.C. §§ 981(a)(1)(C), 982(a), and 28 U.S.C. § 2461(c): Criminal Forfeiture]

The Grand Jury charges:

COUNT ONE

[18 U.S.C. § 1349]

Beginning in or before 2002, and continuing through the date of this indictment, in Los Angeles, Orange, and Riverside counties, within the Central District of California, and elsewhere, defendants YU HAO HUNG, also known as "Alex Young," "Allison Kawai," and "Charlene," and TI LU, also known as "Deer Lu," "Jen Lu," and "Jerry

Young" (collectively, "defendants"), together with others known and unknown to the Grand Jury, conspired to commit bank fraud, in violation of Title 18, United States Code, Section 1344. The object of the conspiracy was carried out, and to be carried out, in substance, as follows: Defendants would obtain the social security numbers of real persons who did not have credit histories and would manipulate their credit scores by adding them as authorized users to credit card accounts with long histories of on-time payments. Defendants would apply for bank-issued credit cards using false information and those stolen social security numbers. Defendants would make purchases with those fraudulently-obtained credit cards, including at fictitious businesses that they controlled. From 2014 through 2017, the conspiracy involved a minimum of 50 different stolen social security numbers, from each of which, as defendant HUNG said in a recorded conversation, defendants expected to generate $100,000 or more in fraudulent proceeds. Federally-insured financial institutions defrauded as a result of this conspiracy include JPMorgan Chase Bank, Ally Bank, Bank of America, Capital One, Everbank, Citibank, and Wells Fargo Bank.

COUNT TWO

[18 U.S.C. § 1028A]

Beginning in or before 2002, and continuing through the date of this indictment, in Los Angeles, Orange, and Riverside counties, within the Central District of California, and elsewhere, defendants YU HAO HUNG, also known as "Alex Young," "Allison Kawai," and "Charlene," and TI LU, also known as "Deer Lu," "Jen Lu," and "Jerry Young", knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person during and in relation to a felony violation of Title 18, United States Code, Section 1349, Conspiracy to Commit Bank Fraud, as charged in Count One.

COUNT THREE

[18 U.S.C. § 1956(h)]

Beginning in or before 2002, and continuing through the date of this indictment, in Los Angeles, Orange, and Riverside counties, within the Central District of California, and elsewhere, defendants YU HAO HUNG, also known as "Alex Young," "Allison Kawai," and "Charlene," and TI LU, also known as "Deer Lu," "Jen Lu," and "Jerry Young" (collectively, "defendants"), together with others known and unknown to the Grand Jury, conspired to launder money, in violation of Title 18, United States Code, Section 1956, namely:

(a) to knowingly conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of a specified unlawful activity, that is bank fraud, with the intent to promote the carrying on of specified unlawful activity, that is bank fraud, and while conducting and attempting to conduct such financial transaction knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i); and

(b) to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, bank fraud, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and while conducting and attempting to conduct such financial transactions knew that the property involved in the financial transactions represented the proceeds of some form of

unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

The objects of the conspiracy were carried out, and to be carried out, in substance, as follows:

(a) Defendants would obtain credit cards from federally-insured financial institutions using false information and the social security numbers of other persons without those other persons' authorization;

(b) Defendants would make false charges on the credit cards at purported businesses that defendants controlled and that, in fact, provided no goods or services;

(c) As defendants knew and intended, as a result of this fraud, federally-insured financial institutions and credit card processors would transfer money into bank accounts that defendants had established for the purported businesses;

(d) Defendants would then transfer the proceeds of their bank fraud from these bank accounts into other bank and brokerage accounts that they also controlled;

(e) Defendants would also use the fraudulently-obtained credit cards to purchase gold, which they would keep in safety deposit boxes and elsewhere, and gift cards in order to store and hide the proceeds of their fraud;

(f) Defendants would sell the gold they obtained by fraud to gold dealers to generate proceeds that could not be traced directly back to their fraud; and

(g) Defendants would use the proceeds of earlier frauds to bribe bank insiders, and to purchase access to social security numbers and mail-receiving services, to enable them to commit new

frauds.

In furtherance of the conspiracy, defendants sent over $1 million of bank fraud proceeds through one of their shell corporations, Nova Diversified Corp, to a purported investment company that defendant HUNG said in a recorded conversation did not report its dividend payments to the Internal Revenue Service.

FORFEITURE ALLEGATION ONE

[18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c) and 18 U.S.C. § 982(a)(2)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given to defendants YU HAO HUNG, also known as "Alex Young," "Allison Kawai," and "Charlene," and TI LU, also known as "Deer Lu," "Jen Lu," and "Jerry Young" (collectively, the "defendants") that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Section 981(a)(1)(C), Title 28, United States Code, Section 2461(c), and Title 18, United States Code, Section 982(a)(2), in the event of any defendant's conviction under Count One or Two of this Indictment.

2. Defendants shall forfeit to the United States the following property:

a. All right, title and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of any offense set forth in Count One or Two of this Indictment including, without limitation:

(i) the funds in TD Ameritrade account number 754-891251 held in the name of TI LU;

(ii) the funds in TD Ameritrade account number 754-382455 held in the name of Jen Lu;

(iii) the funds in Wells Fargo Bank account numbers 9015689558 and 1659652646 held in the name of Nova Diversified Corp, dba Platinum Holdings;

(iv) the funds in Wells Fargo Bank account numbers 3830288928 and 2350252199 held in the name of Alex Young;

(v) the funds in Bank of America account number 501009452585 held in the name of Nova Diversified Corp, dba NDC Designs;

(vi) the funds in Bank of America account number 005012559638 held in the name of Gold World Inc, dba Vintage Reproductions;

(vii) the funds in Bank of America account number 325072566370 held in the name of Allison Kawai;

(viii) the funds in Bank of America account number 000205266404 held in the name of Nova Belle Trust;

(iv) the gold and other valuables stored in the Chase Bank safety deposit boxes located at 270 S. State College Blvd. Brea, CA 92821, which are held in the name of Nova Belle Trust (with Alex Young listed as the trustee);

(v) the real property with Assessor's Parcel Number 931-882-43, commonly known as 18978 Northern Dancer Lane, Yorba Linda, CA 92886, and with title held by Nova Belle Trust, Trustee Alex Young;

(vi) all rights and interest the defendants have personally or through their businesses, corporate entities, and trusts, including Nova Diversified Corp. and Nova Belle Trust, to funds loaned to or invested with Giovanni M. Fernandez, NV Acquisitions, and businesses and corporate entities they own or control, as well as all corresponding interest, dividends, and profits;

(Collectively, the above-described property will be referred to as the "FORFEITABLE PROPERTY"); and

b. A sum of money equal to the total value of the property described in subparagraph a above.

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), and Title 28, United States Code, Section 2461(c), defendants shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of any defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to, or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION TWO

[18 U.S.C. § 982(a)(1)]

1. Pursuant to Rule 32.2, Fed. R. Crim. P., notice is hereby given to defendants YU HAO HUNG, also known as "Alex Young," "Allison Kawai," and "Charlene," and TI LU, also known as "Deer Lu," "Jen Lu," and "Jerry Young" (collectively, the "defendants") that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Section 982(a)(1), in the event of any defendant's conviction under Count Three of this Indictment.

2. Defendants shall forfeit to the United States the following property:

a. All right, title, and interest in any and all property, real or personal, involved in or traceable to any transaction set forth in Count Three of this Indictment, including the FORFEITABLE PROPERTY set forth in Paragraph 2(a) of Forfeiture Allegation One; and

b. A sum of money equal to the total value of the property described in subparagraph a above.

///

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), defendant shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of any defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to, or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

A TRUE BILL

_____

Foreperson

NICOLA T. HANNA
United States Attorney

LAWRENCE S. MIDDLETON
Assistant United States Attorney
Chief, Criminal Division

RANEE A. KATZENSTEIN
Assistant United States Attorney
Chief, Major Frauds Section

ANDREW BROWN
Assistant United States Attorney
Major Frauds Section